UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/713,104	11/15/2000	Eiichi Sato	B422-143	9652

26272 7590 08/20/2008

COWAN LIEBOWITZ & LATMAN P.C.
JOHN J TORRENTE
1133 AVE OF THE AMERICAS
NEW YORK, NY 10036

EXAMINER	
MOORTHY, ARAVIND K	
ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
08/20/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/713,104	SATO, EIICHI	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 June 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *25-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *25-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 November 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the RCE filed on 5 June 2008.

2. Claims 25-29 are pending in the application.

3. Claims 25-29 have been rejected.

4. Claims 1-24 have been cancelled.

Continued Examination Under 37 CFR 1.114

5. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 5 June 2008 has been entered.

Response to Arguments

6. Applicant's arguments with respect to claims 25-28 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 25-29 are rejected under 35 U.S.C. 102(b) as being anticipated by Diamant et al U.S. Patent No. 6,268,789 B1.

As to claim 25, Diamant et al discloses a communication apparatus for transferring data from a first network to a second network, the apparatus comprising:

> a reception unit configured to receive image data via a first network (i.e. According to the present example, communication of confidential information between two nodes can be performed only between nodes which are connected via the secured network 8. For example, when node 40 needs to transfer confidential information to node 20, the confidential information is divided into two elements. The two elements are transmitted from node 40 to node 20 wherein the first element is transmitted over the public network 6 and the second element is transmitted over the secured network 8.) [column 7, lines 33-41];
>
> a first discrimination unit configured to discriminate if the received data is a confidential data (i.e. Thus, information can be stored in the secured storage area 18 in two cases, either if at least partially received from the secured network 8 or if originally determined as confidential information by one of the computers 20, 30 and 40, connected to the secured network 8. It will be appreciated that security is enhanced when all of the secured information is transmitted over the secured network 8.) [column 7, lines 64-67];
>
> a judgment unit configured to judge if security of the transfer path to the destination of the received image data via the second network is ensured or not, when the result of the discrimination by the first discrimination unit indicates the

received data is a confidential data (i.e. For example, retrieving confidential information from the server 4 is performed by transmitting a retrieval request divided into two segments where the first segment is transmitted over the main network 6 and to the destination node and the second segment is transmitted to the destination node over the secured network 8. Hence, only nodes which are connected to the secured network 8 receive the two segments which are required to reconstruct the classified information.) [column 7, lines 4-12];

a first control unit configured to control, when the result of the discrimination by the first discrimination unit indicates the received image data is not confidential, to transfer the received image data to the destination of the received data via the second network regardless of whether security of the transfer path to the destination of the received image data via the second network is ensured or not [column 7, lines 4-12]; and

a second unit configured to control, when the result of the discrimination by the first discrimination unit indicates the received image data is confidential, to transfer the received image data to the destination of the received data via the second network when the result of the judgment by the judgment unit indicates security of the transfer path is ensured, and to store the received image data in a storage area corresponding to the destination of the received image data without transferring the received image data to the destination, when the result of the judgment by the judgment unit indicates security of the transfer path is not ensured (i.e. According to a further storing mode, the managing controller 98

stores the confidential information file in the secured storage area in a segmented form. According to this mode, when requested to retrieve this information from the storage unit 14, the managing controller 98 accesses the segments which form the confidential information file and transmits them without any processing, reassembling and the like.) [column 8, lines 18-25].

As to claim 26, Diamant et al discloses an apparatus, further comprising;

a management unit configured to manage address of a transmission destination in relation with whether there exists a public key (i.e. When the computer system 390 is disconnected from the network 324, the processor 302 retrieves an analysis software application from the secured area, generates a security key and provides the security key to the analysis software. In the present example, the analysis software application is an anti-virus scanning software. Then, the processor 302 provides the analysis software application to the CPU 310. The CPU 310 executes the analysis software application according to the log file on all of the data changes in the public area 318.) [column 10, lines 61-67];

a second discrimination unit configured to discriminate whether there exists the public key related to the address of the transmission destination, if the judgment unit judges that the transfer path is not secure [column 10, lines 61-67];

an encrypting unit configured to encrypt the received data, if the second discrimination unit discriminates that there exists the public key [column 15, lines 1-4]; and

a transmission unit configured to transmit the received data encrypted by the encrypting unit to the transmission destination [column 15, lines 1-4].

As to claim 27, Diamant et al discloses a control method for a communication apparatus for transferring data from a first network to a second network, the method comprising:

receiving image data via a first network (i.e. According to the present example, communication of confidential information between two nodes can be performed only between nodes which are connected via the secured network 8. For example, when node 40 needs to transfer confidential information to node 20, the confidential information is divided into two elements. The two elements are transmitted from node 40 to node 20 wherein the first element is transmitted over the public network 6 and the second element is transmitted over the secured network 8.) [column 7, lines 33-41];

discriminating if the received data is a confidential data (i.e. Thus, information can be stored in the secured storage area 18 in two cases, either if at least partially received from the secured network 8 or if originally determined as confidential information by one of the computers 20, 30 and 40, connected to the secured network 8. It will be appreciated that security is enhanced when all of the secured information is transmitted over the secured network 8.) [column 7, lines 64-67];

judging if security of the transfer path to the destination of the received image data via the second network is ensured or not, when the result of the discrimination indicates the received data is a confidential data (i.e. For example,

retrieving confidential information from the server 4 is performed by transmitting a retrieval request divided into two segments where the first segment is transmitted over the main network 6 and to the destination node and the second segment is transmitted to the destination node over the secured network 8. Hence, only nodes which are connected to the secured network 8 receive the two segments which are required to reconstruct the classified information.) [column 7, lines 4-12];

controlling, when the result of the discrimination indicates the received image data is not confidential, to transfer the received image data to the destination of the received data via the second network regardless of whether security of the transfer path to the destination of the received image data via the second network is ensured or not [column 7, lines 4-12]; and

controlling, when the result of the discrimination indicates the received image data is confidential, to transfer the received image data to the destination of the received data via the second network when the result of the judgment indicates security of the transfer path is ensured, and to store the received data in a storage area corresponding to the destination of the received image data without transferring the received image data to the destination, when the result of the judgment indicates security of the transfer path is not ensured (i.e. According to a further storing mode, the managing controller 98 stores the confidential information file in the secured storage area in a segmented form. According to this mode, when requested to retrieve this information from the storage unit 14,

the managing controller 98 accesses the segments which form the confidential information file and transmits them without any processing, reassembling and the like.) [column 8, lines 18-25].

As to claim 28, Diamant et al discloses a storage medium computer-readably storing a program for causing a computer to execute a control method for a communication apparatus for transferring data from a first network to a second network, the method comprising:

receiving image data via first network (i.e. According to the present example, communication of confidential information between two nodes can be performed only between nodes which are connected via the secured network 8. For example, when node 40 needs to transfer confidential information to node 20, the confidential information is divided into two elements. The two elements are transmitted from node 40 to node 20 wherein the first element is transmitted over the public network 6 and the second element is transmitted over the secured network 8.) [column 7, lines 33-41];

discriminating if the received data is a confidential data (i.e. Thus, information can be stored in the secured storage area 18 in two cases, either if at least partially received from the secured network 8 or if originally determined as confidential information by one of the computers 20, 30 and 40, connected to the secured network 8. It will be appreciated that security is enhanced when all of the secured information is transmitted over the secured network 8.) [column 7, lines 64-67];

judging if security of the transfer path to the destination of the received image data via the second network is ensured or not, when the result of the discrimination indicates the received data is a confidential data (i.e. For example, retrieving confidential information from the server 4 is performed by transmitting a retrieval request divided into two segments where the first segment is transmitted over the main network 6 and to the destination node and the second segment is transmitted to the destination node over the secured network 8. Hence, only nodes which are connected to the secured network 8 receive the two segments which are required to reconstruct the classified information.) [column 7, lines 4-12];

controlling, when the result of the discrimination indicates the received image data is not confidential, to transfer the received image data to the destination of the received data via the second network regardless of whether security of the transfer path to the destination of the received image data via the second network is ensured or not [column 7, lines 4-12]; and

controlling, when the result of the discrimination indicates the received image data is confidential, to transfer the received image data to the destination of the received data via the second network when the result of the judgment indicates security of the transfer path is ensured, and to store the received image data without transferring the received image data to the destination, when the result of the judgment indicates security of the transfer path is not ensured (i.e. According to a further storing mode, the managing controller 98 stores the

> confidential information file in the secured storage area in a segmented form. According to this mode, when requested to retrieve this information from the storage unit 14, the managing controller 98 accesses the segments which form the confidential information file and transmits them without any processing, reassembling and the like.) [column 8, lines 18-25].

As to claim 29, Diamant et al discloses an apparatus, further comprising a transmission unit configured to transmit information to the destination of the received data in a case where the received image data is stored in a storage area [column 8, lines 18-25]. Diamant et al discloses the information indicating that the received image data is stored in the storage area [column 8, lines 18-25].

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aravind K Moorthy/
Examiner, Art Unit 2131
/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2131